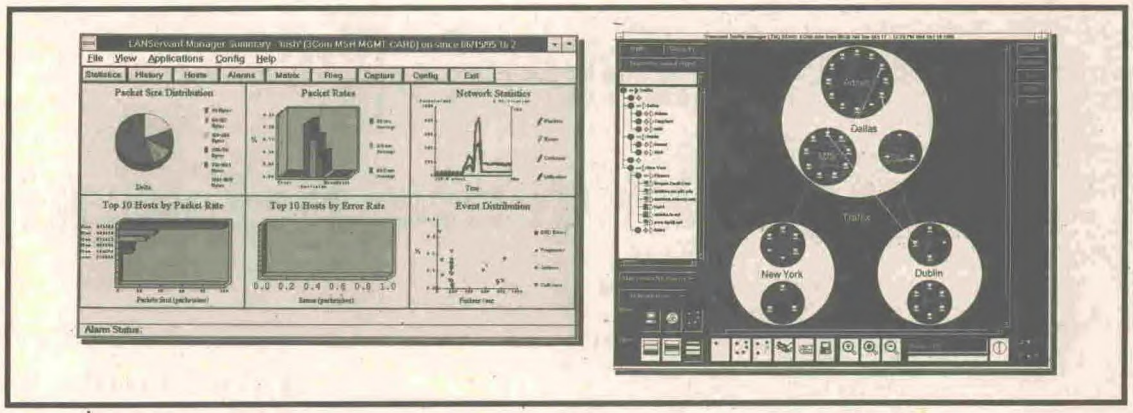
สาทิพย์ กองจันทรา

ระบบเครือข่ายอัจฉริยะ (Intelligence Networking)

เครือข่ายอัจฉริยะจะเป็นระบบเครือข่ายที่สามารถตรวจสอบและ (อาจ) แก้ไขข้อบกพร่องการทำงานต่าง ๆ ของเครือข่ายได้อย่างอัตโนมัติ

การใช้งานระบบเครือข่ายคอมพิวเตอร์นับวันยิ่งจะมีความนิยมใช้งานกันมากขึ้นเรื่อย ๆ จากเพียงไม่กี่บริษัทที่ได้ใช้ระบบเครือข่ายเพื่อรองรับการทำงานภายในบริษัทได้เพิ่มขึ้นเป็นจำนวนมาก ซึ่งแทบทุกบริษัทที่เป็นบริษัทขนาดกลางจนถึงบริษัทขนาดใหญ่จะมีการใช้งานระบบเครือข่ายเสมอ และจากจำนวนเครื่องคอมพิวเตอร์ที่ต่อเชื่อมเป็นระบบเครือข่ายจำนวนไม่กี่สิบเครื่องได้เพิ่มขึ้นเป็นร้อยเป็นพันเครื่องในช่วงระยะเวลาอันรวดเร็ว แต่ด้วยอัตราการเพิ่มขยายของการใช้งานระบบเครือข่ายที่เพิ่มขึ้นอย่างรวดเร็วนั้นทำให้การบริหารและควบคุมการใช้งานต่าง ๆ เหล่านั้นมีความยุ่งยากมากยิ่งขึ้นด้วย และในปัจจุบันอัตราการเพิ่มขยายของบุคลากรที่จะมาทำหน้าที่บริหารและควบคุมระบบเครือข่ายนี้กลับมีอัตราการเพิ่มขยายในอัตราที่ต่ำมากเมื่อเทียบกับการเพิ่มขยายของการใช้งานระบบเครือข่าย โดยเฉพาะในประเทศไทยขณะนี้การขาดแคลนบุคลากรด้านนี้ก็นับว่าเป็นปัญหาที่มีความสำคัญเป็นอย่างมาก งบประมาณของบริษัทในแต่ละปีมีจำนวนไม่น้อยที่ต้องใช้จ่ายไปกับการติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายต่าง ๆ และถึงแม้ว่าจะใช้เงินเป็นจำนวนมากกับการจัดซื้อหรือติดตั้งระบบเครือข่ายไปแล้วก็ตาม ด้วยความแตกต่างระหว่างจำนวนผู้ใช้งานระบบเครือข่ายกับผู้ที่บริหารและควบคุมระบบที่มีความแตกต่างกันเป็นจำนวนมากนั้น ประกอบกับปัจจุบันได้มีเทคโนโลยีและมาตรฐานใหม่ ๆ ที่ได้ถูกคิดค้นพัฒนาขึ้นมาใช้งานกันอย่างมากมาย ทำให้การทำงานและการต่อเชื่อมของระบบเครือข่ายมีความสลับซับซ้อนยากต่อการบริหารและควบคุมมากยิ่งขึ้นอีก



รูปที่ 1 Network Management System

ด้วยเหตุผลของการขยายตัวที่มีความแตกต่างกันมากและความสลับซับซ้อนของเทคโนโลยีในปัจจุบันทำให้บริษัทต่าง ๆ ที่ใช้งานระบบเครือข่ายนั้นต้องสูญเสียค่าใช้จ่ายที่นอกเหนือการคาดหมาย (Hidden Cost) เป็นจำนวนมากในแต่ละปี ซึ่งไม่ว่าจะเป็นค่าใช้จ่ายที่เกิดจากการซ่อมแซมหรือแก้ไขปัญหาของการทำงานระบบเครือข่ายเองที่สามารถเกิดขึ้นได้ทุกเวลา หรือแม้แต่การสูญเสียรายได้อันพึงควรจะได้เนื่องจากบริษัทนั้นไม่สามารถที่จะทำงานปกติของบริษัทต่อไปได้เพราะระบบเครือข่ายคอมพิวเตอร์ที่ใช้รองรับการทำงานไม่สามารถที่จะทำงานได้ตามปกตินั่นเอง จึงทำให้หลายต่อหลายบริษัทได้หันมาให้ความสนใจในเรื่องการบริหารและควบคุมระบบเครือข่ายมากยิ่งขึ้น ได้มีการนำเอาและทดลองใช้เทคโนโลยีใหม่ ๆ เพื่อที่จะช่วยลดค่าใช้จ่ายอันไม่จำเป็นดังกล่าว ทำให้ระบบเครือข่ายที่จะต่อเชื่อมนั้นมีการทำงานที่แตกต่างกว่าเดิมมาก โดยระบบสามารถที่จะบริหารและควบคุมการทำงานต่าง ๆ ได้ง่ายยิ่งขึ้น หรือแม้แต่สามารถที่จะบริหารด้วยการทำงานของระบบเครือข่ายเองระบบเครือข่ายในลักษณะนี้มีชื่อเรียกว่า ระบบเครือข่ายอัจฉริยะ (Intelligence Networking) นั่นเอง

ระบบเครือข่ายอัจฉริยะเป็นระบบเครือข่ายที่ผู้ติดตั้งได้คำนึงถึงการบริหารและการควบคุมการทำงานต่าง ๆ ของระบบเครือข่ายควบคู่กับการต่อเชื่อมของระบบ ซึ่งระบบเครือข่ายอัจฉริยะจะสามารถช่วยลดงานต่าง ๆ ในการที่จะต้องบริหารและควบคุมระบบนั้น ๆ ลดน้อยลงเป็นจำนวนมาก ทำให้วิศวกรผู้ดูแลระบบเครือข่ายคนหนึ่ง ๆ สามารถที่จะบริหารและควบคุมระบบเครือข่ายได้เป็นจำนวนมาก ส่งผลให้บริษัทลดค่าใช้จ่ายได้เป็นอย่างดี ลักษณะของระบบเครือข่ายอัจฉริยะจะเป็นระบบเครือข่ายที่สามารถตรวจสอบและ (อาจ) แก้ไขข้อบกพร่องการทำงานต่าง ๆ ของระบบเครือข่ายได้อย่างอัตโนมัติ ไม่ว่าจะเป็นการทำงานในระดับการทำงานของฟังก์ชันใด ๆ ไม่ว่าจะเป็นระดับสายสัญญาณที่ต่อเชื่อมระดับเครื่องอุปกรณ์ฮาร์ดแวร์ต่าง ๆ หรือแม้แต่การทำงานของซอฟต์แวร์บางชนิด ดังนั้นในระยะเวลาตลอดเกือบสิบปีที่มีการใช้งานระบบเครือข่ายนั้นก็ได้มีการพยายามคิดค้นวิธีและมาตรฐานต่าง ๆ ออกมามากมายเพื่อที่สนองตอบต่อการใช้งานในระบบเครือข่าย ซึ่งในส่วนของการบริหารและควบคุมระบบเครือข่ายก็ได้มีการคิดค้นพัฒนามาตรฐานออกมามากมายเช่นกัน จนในทุกวันนี้ก็ยังคงมีการพัฒนามาตรฐานใหม่ ๆ อยู่เช่นเดิม มาตรฐานที่ได้รับความนิยมกันในช่วงที่ผ่านมาก็มี มาตรฐาน SNMP (Simple Network Management Protocol) และมาตรฐาน CMIP (Common Management Information Protocol) ซึ่งทั้งสองมาตรฐานนี้ถือได้ว่าเป็นพื้นฐานของการบริหารและควบคุมระบบเครือข่ายเลยทีเดียว โดยมาตรฐาน SNMP จะนิยมใช้งานกับระบบเครือข่ายแลน (LAN) และมาตรฐาน CMI นิยมใช้งานกับระบบเครือข่ายระยะไกลหรื เครือข่ายแวน (WAN) ต่อมาได้มีการคิดค้ พัฒนาเพิ่มเติมจากมาตรฐานเดิมจนเกิ มาตรฐานใหม่ขึ้นมาและเริ่มจะได้รับความนิ ใช้งานกันมากยิ่งขึ้นในปัจจุบัน คือ มาตรฐา RMON (Remote Monitoring) และมาตรฐา RMON2

ระบบฟังก์ชันการบริหารระบบเครือข่าย

การบริหารและควบคุมระบบเครือข่ สามารถทำได้โดยการใช้คำสั่งต่าง ๆ ผ่านท ซอฟต์แวร์ที่ติดตั้งที่เครื่องคอมพิวเตอร์เครื่ ใดเครื่องหนึ่ง ซึ่งคำสั่งเหล่านี้จะติดต่อสื่อส กับเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ อื่น ๆ ทำให้สามารถนำข้อมูลต่าง ๆ ที่ติดต่ นั้นมาประมวลผลแสดงค่าสถิติต่าง ๆ ตา ต้องการได้ การแสดงผลหรือข้อมูลที่สื่อสารใ ขบวนการบริหารและควบคุมระบบเครือข่ นั้นค่อนข้างจะมีหลากหลายชนิดวิธี ขึ้นกั บริษัทผู้ผลิตนั้น ๆ จะผลิตสินค้าออกมาใ ลักษณะใด แต่อย่างไรก็ตาม สำหรับระบ เครือข่ายอัจฉริยะทั่ว ๆ ไปทางสถาบันควบคุ มาตรฐานกลางของกลุ่มมาตรฐาน OSI (Op System Interconnect) ได้ออกแบบและข้ แนะนำของการใช้งานฟังก์ชันการบริหารแล

ควบคุมระบบเครือข่าย โดยชื่อว่า ชุดระบบ FCAPS ซึ่งชุดระบบ FCAPS เป็นขอบเขตและฟังก์ชันหลักที่ระบบเครือข่ายอัจฉริยะทั่ว ๆ ไปพึงควรจะมี ซึ่งประกอบด้วยฟังก์ชันหลัก ๆ 5 ฟังก์ชันดังนี้

- ฟังก์ชัน Fault Management
- ฟังก์ชัน Configuration Management
- ฟังก์ชัน Accounting
- ฟังก์ชัน Performance Management
- ฟังก์ชัน Security Management

โดยแต่ละฟังก์ชันจะมีรายละเอียดการทำงานและหน้าที่ที่แตกต่างกัน ดังนี้

1. ฟังก์ชัน Fault Management เป็นฟังก์ชันการทำงานหลักที่ระบบซอฟต์แวร์บริหารเครือข่ายทั่ว ๆ ไปนิยมใช้งานกันเป็นจำนวนมาก เพราะฟังก์ชัน Fault Management จะทำหน้าที่ในการแสดงสัญญาณต่าง ๆ ผ่านทางระบบซอฟต์แวร์เมื่อเกิดความบกพร่องหรือผิดปกติของระบบเครือข่ายเกิดขึ้น โดยบางซอฟต์แวร์สามารถที่จะแก้ไขความบกพร่องบางอย่างของระบบเครือข่ายได้เองอย่างอัตโนมัติ ข้อบกพร่องของระบบเครือข่ายที่จะต้องใช้ฟังก์ชัน Fault Management นี้ เช่น การหยุดการทำงานของอุปกรณ์เครือข่ายใด ๆ การส่งผ่านข้อมูลที่ผิดผ่านอันเกิดจากอุปกรณ์เครือข่ายหรือสายสัญญาณที่ต่อเชื่อมชำรุดและขาด เป็นต้น

2. ฟังก์ชัน Configuration Management ปัจจัยสำคัญอีกปัจจัยหนึ่งของการบริการระบบเครือข่าย คือ การกำหนดและแก้ไขพารามิเตอร์ต่าง ๆ ของอุปกรณ์เครือข่ายที่ใช้ต่อเชื่อมรวมถึงเครื่องคอมพิวเตอร์บางระบบที่ต่อเชื่อมในระบบเครือข่าย ซึ่งมีความจำเป็นอย่างยิ่งกับระบบเครือข่ายขนาดใหญ่ เพราะโดยลักษณะทั่วไปของระบบเครือข่ายขนาดใหญ่แล้วนั้นจะมีการเปลี่ยนแปลงการต่อเชื่อมของระบบเครือข่ายอยู่ตลอดเวลา ซึ่งหมายถึงต้องมีการแก้ไขหรือติดตั้งอุปกรณ์เครือข่ายนั้น ๆ อยู่ตลอดเวลาเช่นกัน ด้วยโครงสร้างของระบบเครือข่ายขนาดใหญ่ที่มีความสลับซับซ้อนของการต่อเชื่อมนั้น การแก้ไขด้วยวิธีพื้นฐานที่ติดตั้งหรือแก้ไขทีละเครื่องตามจุดของเครื่องนั้น ๆ ติดตั้งอยู่จึงไม่สามารถรองรับงานได้ดีพอ จำเป็นต้องมีระบบที่เก็บค่าพารามิเตอร์ทั้งหมดของระบบเครือข่าย และเมื่อต้องการแก้ไขก็สามารถที่จะนำมาแก้ไขได้ง่ายและรวดเร็ว

3. ฟังก์ชัน Accounting ในระบบเครือข่ายบางแห่งโดยเฉพาะระบบเครือข่ายแวนอาจจะต้องมีการควบคุมปริมาณการใช้งานของแต่ละผู้ใช้หรือกลุ่มผู้ใช้ต่าง ๆ เนื่องจากช่องสัญญาณที่ใช้ส่งผ่านเพื่อเชื่อมต่อระหว่างระบบเครือข่ายนั้นจะต้องเสียเงินเพื่อเช่าใช้สายสัญญาณทุก ๆ เดือนเสมอ ซึ่งในปีหนึ่ง ๆ ต้องเสียค่าใช้จ่ายเป็นจำนวนมากกับการเช่าสายสัญญาณนี้ และในระบบซอฟต์แวร์การบริหารและควบคุมระบบเครือข่ายนั้นสามารถที่ทำงานได้โดยใช้ฟังก์ชัน Accounting เป็นฟังก์ชันในการเก็บสถิติการใช้งานต่าง ๆ ของระบบได้ อย่างไรก็ตาม ในระบบเครือข่ายท้องถิ่นหรือระบบเครือข่ายแลนนั้นโดยทั่วไปแล้วระบบจะมีค่าความจุความเร็ว (Bandwidth) ของระบบค่อนข้างสูงมาก ดังนั้นฟังก์ชันนี้จึงไม่ค่อยมีความจำเป็นนักในระบบเครือข่ายแลน

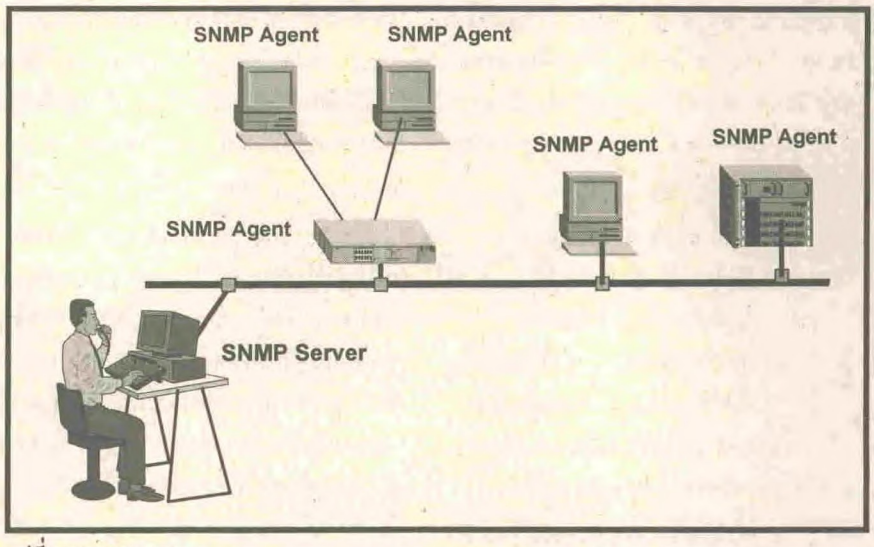
4. ฟังก์ชัน Performance Management นับเป็นฟังก์ชันที่วิศวกรผู้บริหารเครือข่ายมักจะคำนึงถึงก่อนเสมอทั้ง ๆ ที่ฟังก์ชันการบริหารประสิทธิภาพของระบบเครือข่ายนี้ควรจะถูกนำมาใช้งานก็ต่อเมื่อวิศวกรคนนั้นสามารถบริหารและควบคุมการทำงานของระบบเครือข่ายในเบื้องต้นได้เป็นอย่างดีและเรียบร้อยแล้ว และปัจจุบันเองในระบบเครือข่ายแลนนั้นมีเทคโนโลยีใหม่ ๆ ที่สามารถรองรับความเร็วในการส่งผ่านข้อมูลของระบบเครือข่ายได้ที่ความเร็วสูงมากถึงในระดับความเร็วที่ร้อยล้านบิตต่อวินาที (Gigabit Network) เลยทีเดียว แต่ในขณะที่ความเร็วของระบบเครือข่ายแวนมีความเร็วสูงสุดเพียงความเร็วที่ 64 กิโลบิตต่อวินาทีหรือที่ความเร็ว 2 เมกะบิตต่อวินาทีเท่านั้น ดังนั้นฟังก์ชันการบริหารประสิทธิภาพของระบบเครือข่ายจึงมีความสำคัญอย่างยิ่งเฉพาะในระบบเครือข่ายแวนมากกว่าในระบบเครือข่ายแลน

5. ฟังก์ชัน Security Management ระบบความปลอดภัยของระบบเครือข่ายเริ่มมีความสำคัญอย่างมากเมื่อมีการต่อเชื่อมระบบเครือข่ายเข้ากับระบบเครือข่ายของหน่วยงานอื่น ๆ โดยเฉพาะการต่อเชื่อมเข้ากับระบบอินเทอร์เน็ต เพราะเป็นการต่อเชื่อมเข้ากับระบบเครือข่ายสาธารณะที่ใคร ๆ ก็สามารถที่จะสื่อสารข้อมูลไปได้ทุกแห่งหนทั่วโลกของระบบอินเทอร์เน็ต ระบบความปลอดภัยของระบบเครือข่ายมีความสำคัญอย่างยิ่งเพื่อป้องกันการลักลอบการตรวจสอบหรือแก้ไขข้อมูลของบริษัทโดยไม่ได้รับอนุญาต ซึ่งอาจนำความเสียหายอย่างรุนแรงต่อบริษัทได้ ดังนั้นในสภาวะการขยายตัวของระบบเครือข่ายในปัจจุบันนี้ฟังก์ชันความปลอดภัยของระบบเครือข่ายจึงมีความจำเป็นอย่างยิ่งในการบริหารและควบคุมระบบเครือข่าย

SNMP มาตรฐานระบบบริหารเครือข่าย

ด้วยความต้องการที่จะบริหารและควบคุมการทำงานต่าง ๆ ของระบบเครือข่ายได้อย่างมีประสิทธิภาพโดยที่มีพนักงานหรือวิศวกรที่ดูแลงานด้านนี้ไม่กี่คนนั้น ก็ได้มีการพยายามคิดค้นพัฒนาเทคโนโลยีใหม่สำหรับในด้านการบริหารและควบคุมระบบเครือข่ายโดยเฉพาะ ซึ่งระบบการทำงานนี้จะทำให้ผู้บริหารเครือข่ายสามารถที่จะบริหารและควบคุมการทำงานของอุปกรณ์เครือข่ายต่าง ๆ จำนวนมากในระบบเครือข่ายได้อย่างสะดวกและรวดเร็ว โดยจะทำงานผ่านทางจอมอนิเตอร์ของเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งในระบบเครือข่าย เครื่องคอมพิวเตอร์นี้จะมีการติดต่อสื่อสารข้อมูลบางอย่างกับอุปกรณ์เครือข่ายต่าง ๆ ในระบบดังรูปที่ 2 ซึ่งระบบหรือวิธีของการสื่อสารข้อมูลนี้ก็คือมาตรฐานต่าง ๆ ที่ได้คิดขึ้นมานั่นเอง โดยมาตรฐานที่นิยมใช้กันมากคือ มาตรฐาน SNMP (Simple Network Management Protocol)

ดังนั้นอาจกล่าวได้ว่าการที่จะสามารถบริหารและควบคุมการทำงานของอุปกรณ์เครือข่ายใด ๆ ในระบบเครือข่ายนั้นได้ อุปกรณ์เครือข่ายนั้น ๆ จะต้องรองรับการทำงานตามมาตรฐาน SNMP ได้ โดยมักจะเรียกอุปกรณ์เหล่านั้นว่า SNMP Client และในส่วนของระบบซอฟต์แวร์ที่จะติดตั้งในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งเพื่อเป็นส่วนติดต่อกับผู้บริหารเครือข่ายนั้นจะประกอบด้วย 2 ส่วนคือ ส่วนฟังก์ชันของ SNMP Server ซึ่งจะทำหน้าที่สื่อสารและแลกเปลี่ยนข้อมูลกับ SNMP Client ต่าง ๆ และในส่วนแสดงผลของข้อมูลที่ได้คำนวณด้วยฟังก์ชัน SNMP Server ซึ่งในการแสดงผลข้อมูลต่าง ๆ นี้จะไม่มีมาตรฐานในการแสดงผลที่แน่นอน ดังนั้นรูปภาพหรือกราฟที่แสดงออกก็จะมีความแตกต่างกันไปตามชนิดหรือบริษัทผู้ผลิตซอฟต์แวร์นั้น ๆ โครงสร้างการทำงานของมาตรฐานโปรโตคอล SNMP จะเป็นการสื่อสารข้อมูลโดยแบ่งชนิดข้อมูลต่าง ๆ ออกเป็นหมวดหมู่ที่เรียกว่า ฐานข้อมูล MIB (Management Information Base) โดยในแต่ละฐานข้อมูลก็จะบรรจุข้อมูลแต่ละชนิดของการทำงานแตกต่างกันออกไป เช่น ฐานข้อมูลของค่าความผิดพลาดต่าง ๆ ของอินเตอร์เฟสของอุปกรณ์ (Interface MIB) หรือฐานข้อมูลของค่าไอพีแอดเดรส (IP MIB) เป็นต้น ซึ่งในวิวัฒนาการของการพัฒนาระบบฐานข้อมูล MIB นี้ ณ ปัจจุบันมีอยู่ด้วยกัน 2 กลุ่ม คือ ฐานข้อมูล MIB I และฐานข้อมูล MIB II โดยฐานข้อมูล MIB II เป็นการพัฒนาเพิ่มเติมจากฐานข้อมูล MIB I นั่นเอง

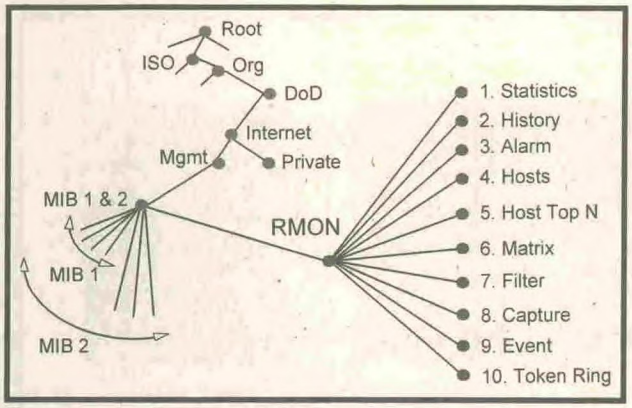


รูปที่ 2 SNMP System

RMON/RMON2 มาตรฐานใหม่สำหรับการบริหารเครือข่าย

ด้วยโครงสร้างการต่อเชื่อมระบบเครือข่ายที่มีขนาดใหญ่และมีความสลับซับซ้อนมากยิ่งขึ้นในปัจจุบัน ทำให้ระบบการทำงานของมาตรฐานโปรโตคอล SNMP ไม่สามารถจะรองรับการทำงานบริหารและควบคุมระบบเครือข่ายได้ดีพอ เพราะพื้นฐานการทำงานของมาตรฐานโปรโตคอล SNMP มีองค์ประกอบอยู่สองส่วนคือ ฟังก์ชัน SNMP Agent และฟังก์ชัน SNMP Server เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น SNMP Server จะคอยส่งสัญญาณตรวจสอบ (Polling) และขอข้อมูลจาก SNMP Agent แล้วนำมาแสดงผลเป็นรูปลักษณะต่าง ๆ บนหน้าจอมอนิเตอร์ของเครื่องคอมพิวเตอร์นั้น ๆ และด้วยเหตุที่ฟังก์ชัน SNMP Server มีการทำงานในลักษณะคอยส่งสัญญาณตรวจสอบ (Polling) ก่อนที่จะได้ข้อมูลจาก SNMP Agent นั้นมาแสดงผล ดังนั้นถ้าต้องการข้อมูลของระบบเครือข่ายอย่างถูกต้องและรวดเร็วตามเวลาทุก ๆ นาทีหรือทุก ๆ ชั่วโมง ก็จะต้องสั่งกำหนดให้ SNMP Server ส่งสัญญาณตรวจสอบออกไปในระบบเครือข่ายทุก ๆ นาทีหรือทุก ๆ ชั่วโมง ซึ่งการทำงานในลักษณะเช่นนี้ทำให้ไม่สามารถที่จะรองรับการบริหารและควบคุมระบบเครือข่ายได้ดีพอ เพราะการที่ทำให้ SNMP Server ส่งสัญญาณตรวจสอบออกไปในระบบเครือข่ายเป็นจำนวนมากนั้นจะทำให้ประสิทธิภาพการสื่อสารข้อมูลในระบบเครือข่ายลดลงได้ และการที่ระบบมาตรฐานโปรโตคอลออกแบบให้ SNMP Server เป็นฟังก์ชันที่รวบรวมข้อมูลทุกอย่างจาก SNMP Agent ของทุกเครื่องแล้วคำนวณวิเคราะห์และแสดงผลโดยเครื่องคอมพิวเตอร์เดียวนั้น ทำให้เมื่อระบบเครือข่ายมีขนาดใหญ่ประกอบด้วยเซกเมนต์เป็นจำนวนมากและถ้าจะต้องคำนวณวิเคราะห์และแสดงผลของระบบเครือข่ายหลาย ๆ เซกเมนต์หรือทั้งหมดพร้อม ๆ กันนั้น เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น SNMP Server จะไม่สามารถรองรับการทำงานได้ดีพอและจะต้องใช้เครื่องคอมพิวเตอร์ที่มีขนาดใหญ่มาก ๆ ทั้งฮาร์ดดิสก์ (Harddisk) และหน่วยความจำ (Memory) ซึ่งจะทำให้ราคาของเครื่องคอมพิวเตอร์เครื่องนี้มีราคาที่สูงมาก

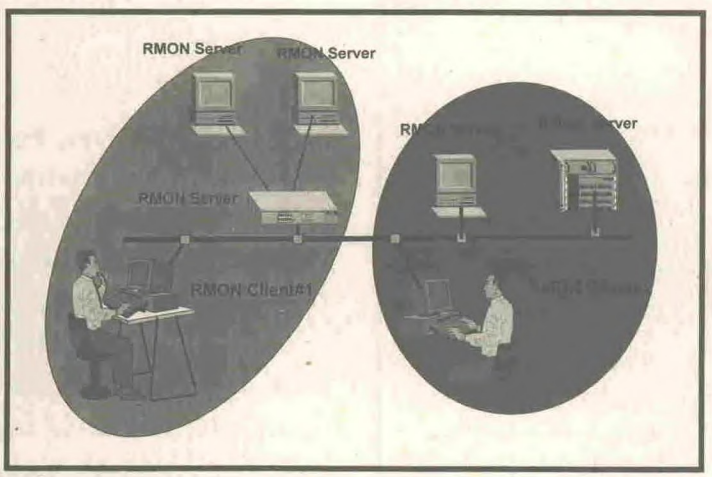
ด้วยเหตุผลของการขยายตัวของระบบเครือข่ายทำให้มีการคิดค้นมาตรฐานใหม่สำหรับการบริหารและควบคุมระบบเครือข่ายเกิดขึ้น ซึ่งในปี ค.ศ. 1991 สถาบัน IETF (Internet Engineering Task Force) ได้ประกาศมาตรฐานที่เรียกว่า โปรโตคอล RMON (Remote Monitoring) โดยมาตรฐานโปรโตคอลนี้มีโครงสร้างของฐานข้อมูล MIB เช่นเดียวกับมาตรฐาน SNMP ดังรูปที่ 3 ซึ่งโปรโตคอล RMON ได้แบ่งกลุ่มของฐานข้อมูลออกเป็นทั้งหมด 9 กลุ่มสำหรับระบบอีเธอร์เน็ต (Ethernet) และ 10 กลุ่มสำหรับระบบโทเก้นริง (Token Ring) ดังรูปที่ 4 องค์ประกอบการทำงาน



รูปที่ 3 Diagram of RMON MIB

❶Statistics - Traffic and error rates on a segment
❷History - Above statistics with a time stamp
❸Alarm - User defined threshold alarms on any RMON variable
❹Hosts - Traffic and error rates for each host by MAC address
❺Host Top N - Sorts hosts by top traffic and/or error rates
❻Matrix - Conversation matrix between hosts
❼Filter - Definition of what packet types to capture and store
❽Packet Capture - Creates a capture buffer on the probe that can be requested and decoded by the management application
❾Event - Generates log entries and/or SNMP traps
❿Token Ring - Token Ring extensions, most complex group

รูปที่ 4 RMON MIB Groups

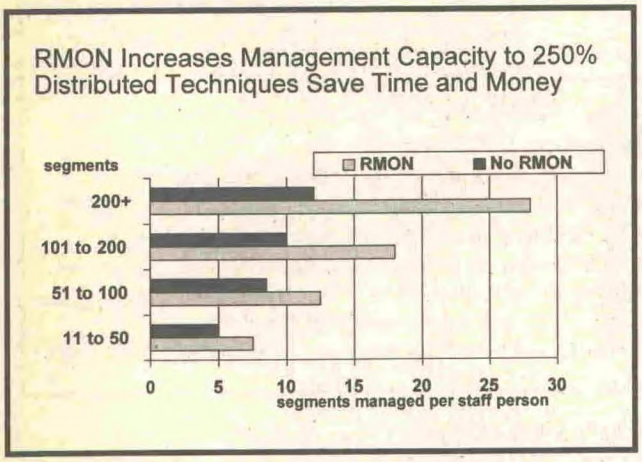


รูปที่ 5 RMON System

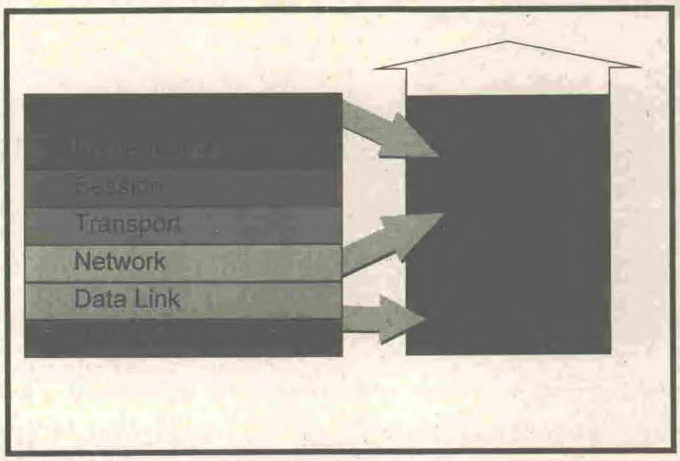
ของโปรโตคอล RMON มีองค์ประกอบคล้ายกับโปรโตคอล SNMP คือประกอบด้วยฟังก์ชัน RMON Server และฟังก์ชัน RMON Client โดยฟังก์ชัน RMON Server จะติดตั้งอยู่ในอุปกรณ์เครือข่ายต่าง ๆ ซึ่งในระบบโปรโตคอล SNMP จะทำงานด้วยฟังก์ชัน SNMP Agent และในทำนองเดียวกันเครื่องคอมพิวเตอร์ที่ผู้บริหารเครือข่ายใช้บริหารและควบคุมระบบเครือข่ายนั้นจะทำงานด้วยฟังก์ชัน RMON Client แทน โดยสำหรับระบบโปรโตคอล SNMP ก็จะทำงานฟังก์ชัน SNMP Server ดังนั้นเครื่องคอมพิวเตอร์ที่ทำงานด้วยฟังก์ชัน RMON Client นี้จึงไม่จำเป็นต้องเป็นเครื่องคอมพิวเตอร์ที่มีคุณสมบัติต่าง ๆ สูงเหมือนกับเครื่องคอมพิวเตอร์ที่ทำงานด้วยฟังก์ชัน SNMP Server และยังสามารถที่จะมีเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น RMON Client ได้หลายเครื่องในระบบเครือข่ายเดียวกันได้ โดยที่ในแต่ละเครื่องอาจกำหนดให้แสดงผลของแต่ละกลุ่มของเครือข่ายหรือชนิดของอุปกรณ์เครือข่ายที่ต้องควบคุมโดยเฉพาะงานนั้น ๆ ได้ดังรูปที่ 5

ด้วยโครงสร้างการทำงานของโปรโตคอล RMON ทำให้สามารถรองรับการบริหารและควบคุมระบบเครือข่ายขนาดใหญ่ได้อย่างมีประสิทธิภาพ ซึ่งจะช่วยให้ลดค่าใช้จ่ายในการบริหารและควบคุมระบบเครือข่ายได้เป็นอย่างดี หรือแม้แต่ค่าใช้จ่ายที่นอกเหนือการคาดหมายนั้น (Hidden Cost) ก็ยังสามารถช่วยลดค่าใช้จ่ายได้เป็นอย่างดีดังรูปที่ 6 เป็นการเปรียบเทียบกราฟสัมพันธ์ระหว่างจำนวนวิศวกรผู้ดูแลระบบเครือข่ายหรือค่าใช้จ่ายในการดูแลระบบเครือข่ายนั้นกับขนาดของระบบเครือข่าย ซึ่งจะเห็นได้ว่าเมื่อระบบเครือข่ายมีขนาดใหญ่มากขึ้นไปนั้น ฟังก์ชันการทำงานของมาตรฐานโปรโตคอล RMON จะน้อยกว่าการทำงานด้วยฟังก์ชันอื่น ๆ เป็นจำนวนมาก

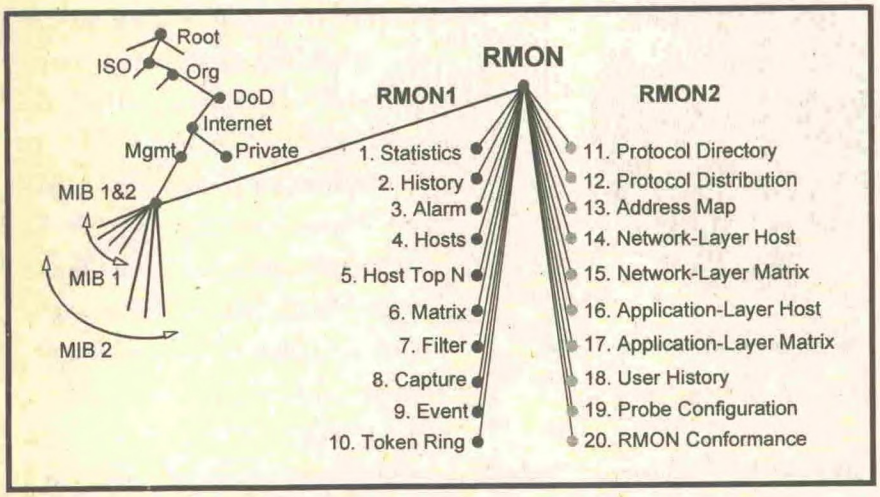
หลังจาก 3 ปีให้หลังที่ได้มีการประกาศใช้มาตรฐานโปรโตคอล RMON ก็ได้มีการริเริ่มพัฒนาระบบมาตรฐานใหม่คือ ได้เพิ่มประสิทธิภาพการทำงานของโปรโตคอล RMON ให้มากยิ่งขึ้นอีก ซึ่งได้เป็นมาตรฐานใหม่ที่เรียกว่า มาตรฐานโปรโตคอล RMON2 โปรโตคอล RMON2 เป็นโปรโตคอลที่มีการทำงานด้วยฟังก์ชันการบริหารและควบคุมระบบเครือข่ายในระดับชั้นฟังก์ชันเลเยอร์ (OSI-Layer) ที่ใกล้เคียงกับระบบซอฟต์แวร์มากยิ่งขึ้น คือจากเดิมที่โปรโตคอล RMON จะทำงานในระดับฟังก์ชันของสายสัญญาณ (Physical Layer) และชั้นฟังก์ชันดาต้าลิงค์ (Datalink Layer) เท่านั้น สำหรับโปรโตคอล RMON2 จะมีการทำงานในระดับฟังก์ชันตั้งแต่ชั้นฟังก์ชันเน็ตเวอร์กเลเยอร์ (Network Layer) ขึ้นไปดังรูปที่ 7 เป็นการเปรียบเทียบชั้นฟังก์ชันต่าง ๆ กับมาตรฐานโปรโตคอล RMON และ RMON2 และในปัจจุบันทางสถาบัน IETF ได้ประกาศโปรโตคอล RMON2 เป็นมาตรฐานสากลเมื่อเดือนมกราคมที่ผ่านมา คือมาตรฐาน RFC 2021 และมาตรฐาน RFC 2027



รูปที่ 6 Using RMON, Network Management Staff Can Provide Services to More Users and Segments



รูปที่ 7 Remote Monitoring in the ISO Model Going Up-the-stack With RMON2



รูปที่ 8 Diagram of the RMON2 MIB

เพิ่มประสิทธิภาพระบบเครือข่ายอัจฉริยะ

การบริหารและควบคุมระบบเครือข่ายนอกจากจะใช้การทำงานด้วยมาตรฐานโปรโตคอล SNMP; RMON และ RMON2 แล้ว ผู้บริหารเครือข่ายใด ๆ สามารถที่จะนำเอาเทคโนโลยีหรือเทคนิคใหม่ ๆ เข้ามาใช้งานในระบบเครือข่ายได้ เพราะในปัจจุบันได้มีการคิดค้นเทคนิคและวิธีการใหม่ ๆ สำหรับการบริหารและควบคุมระบบเครือข่ายขึ้นมามากมาย ซึ่งถึงแม้ว่าวิธีนั้นจะเป็นฟังก์ชันที่คิดค้นโดยบริษัทผู้ผลิตบริษัทใดบริษัทหนึ่งก็ตาม แต่ด้วยความมีประสิทธิภาพและได้รับความนิยมกันมากก็สามารถที่จะนำมาใช้งานหลักกับระบบเครือข่ายได้เป็นอย่างดี อาทิเช่น การบริหารและควบคุมค่าไอพีแอดเดรส (IP Address) ของระบบเครือข่ายที่ทำงานด้วยมาตรฐานโปรโตคอล TCP/IP หรือระบบเครือข่ายอินทราเน็ตก็มีมาตรฐานที่เรียกว่า DHCP (Dynamic Host Config Protocol) ซึ่งเป็นมาตรฐานที่พัฒนามาจากมาตรฐาน BOOTP โดยมีจุดประสงค์ในการบริหารค่าไอพีแอดเดรสโดยเฉพาะ และสำหรับระบบเครือข่ายสมัยใหม่ที่นำเอาเทคโนโลยีสวิตชิง (Switching Network) เข้ามาใช้งานกันนั้นก็สามารถที่จะนำเอาเทคนิค VLAN (Virtual LAN) เข้ามาใช้งานได้เป็นอย่างดี นอกจากนั้นการที่ทำให้อุปกรณ์เครือข่ายบางชนิดเดิมที่มีขั้นตอนการติดตั้งและควบคุมที่ยุ่งยากมากนั้น เช่น อุปกรณ์เราเตอร์ (Router) สามารถที่จะติดตั้งได้ง่ายเช่นเดียวกับอุปกรณ์พื้นฐานดังเช่น ฮับหรือรีพีตเตอร์ (HUB/Repeator) ด้วยวิธีที่เรียกว่า Plug-and-Play ก็จะสามารถช่วยลดค่าใช้จ่ายได้เป็นอย่างดี